REMARKS/ARGUMENTS

Applicants cancel non-method claims 18 and 20-43. Applicants submit that this amendment canceling claims should be entered because amendments canceling claims after a final rejection are permitted. See, 37 CFR 1.116(b)(1), MPEP 714.12.

1. Applicants Request Examiner Initial Reference on Previously Submitted IDS

Attached hereto is a copy of an Information Disclosure Statement (IDS), Form 1449, originally filed on September 6, 2002, including Examiner initials of references the Examiner presented in the First Office Action dated Nov. 16, 2004. The Examiner did not initial the reference at the top of page 2 of the attached IDS. Applicants request the Examiner to initial the reference on page 2 of the 1449 to indicate that all references were reviewed.

2. Claims 1-17 are Patetentable Over the Cited Art

The Examiner rejected claims 1-17 as obvious (35 U.S.C. §103(a)) over Shear (U.S. Patent Pub. 2001/0042043) and O'Connor (U.S. Patent No. 5,745,568). Applicants traverse.

Claim 1 recites a method for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into an interface device, and require: providing an association of at least one coding key to the plurality of storage cartridges; encrypting the coding key; receiving, by the interface devices, an Input/Output (I/O) request; decrypting, by the interface devices, the encrypted coding key in response to the I/O request to use to decode data to be read and code data to be written with respect to the storage medium of the at least one storage cartridges to perform the received I/O request. These claims were amended to recite that interface devices decrypt the encrypted coding key to use to decode and code data for the storage cartridges.

The Examiner recognized the deficiencies of Shear and cited col. 4, lines 2-16 of O'Connor to overcome these deficiencies. (Office Action, pgs. 2-3) Applicants submit that the cited O'Connor is similarly deficient for the following reasons.

The cited col. 4 of O'Connor discusses a technique to install a program from a CD-ROM onto a computer system. The CD-ROM access program runs a hardware identifier routine that retrieves the hardware identifier associated with a customer's computer system. A verify software hardware step reads the hardware identifier written to a loaded CD ROM, compares the hardware identifier of the computer and the CD-ROM. If they match, a routine decrypts the

software files using the hardware identifier as a decryption keys. The decrypted files are then installed.

Nowhere does the cited col. 4 of O'Connor teach or suggest the claim requirements of decrypting the encrypted coding key in response to an I/O request to use to decode data to be read and code data to be written with respect to the storage medium of the target storage cartridge to perform the received I/O request. Instead, the cited O'Connor discusses decrypting files if identifiers match and then installing the decrypted files. There is no teaching or mention of the claim requirement of decrypting a key for an I/O request to code data to be written to perform the I/O request. Further, nowhere is there any teaching that multiple interface devices decrypt the encrypted coding key to use to code data to write to the storage cartridges.

Applicants further submit that O'Connor is deficient for the reasons discussed with respect to Shear in that both discuss techniques to use to decrypt data. Nowhere do these references alone or in combination teach or suggest the claim requirements of decrypting the encrypted coding key in response to an I/O request to use to code data to be written to perform the received I/O request. Further, nowhere is there any teaching that multiple interface devices decrypt the encrypted coding key to use to code data to write to the storage cartridges.

Accordingly, for the above reasons, Applicants submit that the independent claim 1 is patentable over the cited art because the cited Shear does not disclose all the claim requirements.

Claims 2-9 are patentable over the cited art because they depend from claim 1, which is patentable over the cited art for the reasons discussed above. Moreover, the below discussed independent claims provide additional grounds of patentability over the cited art.

Claim 8 depends from claim 1 and further requires that encrypting the coding key further comprises: encrypting the coding key with a first key, wherein a second key is used to decrypt the coding key encrypted with the first key; encrypting the second key with a third key, wherein a fourth key is used by the interface device to decrypt data encrypted with the third key; and transmitting the coding key encrypted with the first key and the second key encrypted with the third key to the interface device.

The Examiner cited FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear as disclosing the requirements of the pre-amended claims. (FOA, pgs. 4-5) Applicants traverse with respect to the amended claims.

The cited para. 0078 discusses rights management to exchange movies and games. Content is encrypted with decryption keys required to decrypt the content. The decryption keys

may themselves be encrypted in an encrypted key block. The cited para. 0079 mentions that content may be secured as it is recording, such as in a camera. Reading the content for use in the rights management environment might occur at many steps along a conventional production and distribution process. Para. 0080 mentions that the storage medium carries the decryption key in a hidden portion that is used by a drive to decrypt the encrypted key block. The cited para. 0081 mentions that the video disk drive may store keys to decrypt an encrypted key block or the may be stored in a drive key store and be updateable.

The cited paras. 0127-0138 mention that different information on the medium may be encrypted using different keys and that encrypted keys may be stored on the medium to be used to decrypt the protected properties and metadata. Multiple sets of encrypted keys may be stored on the medium to have different keys associated with different regions. A decryption key for the encrypted keys may be hidden on the medium.

The cited para. 0183 mentions that a disk may store properties or other content in protected or unprotected form, where a property is protected if it is at least in part encrypted. The disk could store both a movie as protected property and an unprotected interview, and store any number of protected or unprotected properties.

The cited paras. 0193-0199 discuss local secure execution of a control process and the use of optical media. Special hardware can be used to provide a secure execution environment to ensure safe digital commerce activities. A metering and control system, at least partially encrypted, is delivered to a user on optical media. A bill may be generated in response to transmitting information. Some or all of the content may be encrypted on the media.

The cited paras. 0216-0220 further discusses that the disk may store an encrypted key block used to decrypt properties and metadata on the disk, where different keys may be used for different data on the disk. The cited para. [0217] mentions that the cryptographic key block, which is the key used to decrypt the data, may be encrypted with one or more additional keys, and that these one or more keys need to be used to decrypt the key block to obtain the key to decrypt the data. The cited paras. [0218-0220] mentions that the keys to decrypt the encrypted key block may come from different sources. The disk may store hidden keys or the keys may be provided by the disk drive. The disk drive may have an integrated circuit decryption engine including a small secure internal key store memory having keys to use to decrypt the encrypted key block, which is then used to decrypt the content. The keys to decrypt the protected content may also be within a secure container.

The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Although the cited Sheer discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that teaches encrypting the key used to decrypt the coding key with a third key, and that the interface device, or cited drive, uses a fourth key the key that is then used to decrypt the coding key, or cited encrypted key block. Further, the Examiner has not cited any part of Shear that discloses transmitting the decryption key encrypted with a first key and the second key encrypted with a third key to the interface device. In other words, the Examiner has not cited any part of Shear that teaches encrypting the key used to decrypt the coding key.

Accordingly, Applicants submit that claim 8 provides additional grounds of patentability over the cited art because the cited Shear and O'Connor do not teach the additional requirements of these claims.

Claim 9 depends from claim 6 and further requires that encrypting the coding key comprises: encrypting the coding key with a first key, wherein a second key is used to decrypt the coding key encrypted with the first key; transmitting the coding key encrypted with the first key to the interface device; receiving, from the interface device, the coding key encrypted with the first key; decrypting the coding key with the second key; encrypting the coding key with a third key, wherein a fourth key is used by the interface device to decrypt data encrypted with the third key; and transmitting the coding key encrypted with the third key to the interface device.

The Examiner cited the above discussed sections of Shear with respect to these claims. (FOA, pg. 5). The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Although the cited Sheer discusses encrypting a decrypting key used to decrypt content on the disk with on or more keys, the Examiner has not cited any part of Shear that teaches

receiving the coding key encrypted with a first key from the interface device, decrypting the coding key with a second key, reencrypting the coding key with a third key and transmitting that reencrypted coding key to the interface device, which uses a fourth key to decrypt. For instance, the Examiner has not cited any part of Shear that discloses that the DVD drive transmits the encrypted coding key to another device that decrypts that key and reencrypts with a key with a yet further key that the drive can decrypt.

Accordingly, Applicants submit that claim 9 provides additional grounds of patentability over the cited art because the cited Shear does not teach the additional requirements of these claims.

Independent claim 10 recites a method performed by an interface device for accessing data in a performed by an interface device for accessing data in a removable storage cartridge including a read/write storage medium coupled to the interface device, and require: receiving an encrypted coding key from a host system with an Input/Output (I/O) request; decrypting the encrypted coding key; using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request; using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and storing the received encrypted coding key in the storage medium to use for subsequent I/O requests.

The Examiner cited the above discussed FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear as disclosing the requirements of the pre-amended claims. (FOA, pg. 5)

Applicants submit that the Examiner has not cited any part of Shear that teaches or suggests an interface device for accessing a coupled storage medium receive an encrypted key from a host with an I/O request to decrypt and use to encode data to write to the storage medium for a write I/O request and decode data read from the storage for a read I/O request. Instead, as discussed, the cited Shear discusses a drive accessing an encrypted decrypting key to use to decrypt content on a disk (DVD). This does not disclose decrypting the decrypted encoding key to use encode data to write to the storage medium for an I/O request.

Further, the Examiner has not cited any part of Shear that teaches the claim requirement of storing the received encrypted coding key in the storage medium to use for subsequent I/O requests. The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the

disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys. However, these cited sections do not disclose that the disk drive, which decrypted and used a key to code data to write to the storage, stores the received encrypted coding key in the storage medium for subsequent I/O requests.

Accordingly, for the above reasons, Applicants submit that the independent claim 10 is patentable over the cited art because the cited Shear does not disclose all the claim requirements.

Claims 11-17 are patentable over the cited art because they depend from claims 10, which is patentable over the cited art for the reasons discussed above. Moreover, the below discussed dependent claims provide additional details grounds of patentability over the cited art.

Claim 16 depends from claim 10 and further require that the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key to decrypt data encrypted using the first key. These claims additionally require: receiving, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key; accessing the fourth key; using the fourth key to decrypt the encrypted second key received from the host system; and using the decrypted second key to decrypt the received coding key encrypted using the first key.

The Examiner cited the above discussed sections of Shear with respect to these claims. (FOA, pgs. 6-7)

Applicants submit that the Examiner has not cited any part of Shear that teaches that the coding key, corresponding to the cited decryption key, is encrypted with a first key and that the interface device receives a second key encrypted with a third key that it decrypts with a fourth key to then use the second key to decrypt encrypted coding key to use. For instance, the Examiner has not cited where Shear discloses that the disk drive receives a further key that is used to decrypt the key it maintains to use to decrypt the key block on the DVD. Instead, the cited Shear, including para. 0217 mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Accordingly, Applicants submit that claim 16 provides additional grounds of patentability over the cited art because the cited Shear does not disclose the additional requirements of these claims.

Claim 17 provides additional grounds of patentability over the cited art for the reasons discussed with respect to claim 16 because claim 17 concerns the use of third and fourth keys to encrypt and decrypt a second key that may be used to decrypt the coding key that is used to encode and code data.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-17 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: June 24, 2008

By:_____/David Victor/_____

David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984

FORM PTO-1449

INFORMATION DISCLOSURE CITATION IN AN APPLICATION

(Use several sheets if necessary)

Docket Number	Application Number
TUC920010022US1	09/977,159
Applicant G.A. Jaquette	
Filing Dat October 11, 2001	**Group Art Unit** 2161

U.S. PATENT DOCUMENTS

EXAMINER INITIAL	DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
F.B	Re. 36181	04/06/99	Koopman, Jr. et al.			
	4799061	01/17/89	Abraham et al.			
	5285497	02/08/94	Thatcher, Jr.			
	5319701	06/07/94	Atalla et al.			
	5321749	06/14/94	Virga			
	5398283	03/14/95	Virga			
	5416846	05/16/95	Merrick			
	5475121	12/26/95	Weiss			
	5642421	06/24/97	Gray et al.			
	5719938	02/17/98	Haas et al.			
	5800570	09/08/98	Nardone et al.			
	5809145	09/15/98	Slik et al.			
	5915021	06/22/99	Herlin et al.			
	5956404	09/21/99	Slavin			
	5963635	10/05/99	Goldstein			
	5970144	10/26/99	Brandman			
	5974399	11/23/99	Aucsmith et al.			
	6134658	08/15/00	Braithwaite et al.			
F.B	6219789	04/17/01	Jaquette			

FOREIGN PATENT DOCUMENTS

	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation YES	Translation NO
F.B	0924895	06/23/99	EP			Abstract	
F.B	9848389	10/29/98	PCT			Abstract	

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

F.B	U.S.Patent Application Serial No. 09/977,161, filed on October 11, 2001, entitled, "Method, System, and Program, for Encoding Decoding Input Data", invented by G.A. Jaquette.
	Microsoft Corp., "Encrypting File System for Windows 2000." Copyright 1998 Microsoft Corporation
	IBM, Corp., "A Fast Hardware Data Compression Algorithm and Some Algorithmic Extensions", Journal of Research and Development, Vol. 42, No. 6, 1998, pp. 1-13.
	Lewis, Harry A. and Larry Denenberg. "Lempel-Ziv Encoding." in: *Data Structures & Their Algorithms*. Harper Collins Publishers 1991.
F.B	Quarter-Inch Cartridge Drive Standards, Inc., "Adaptive Lossless Data Compression (ALDC)", QIC-154, Revision A, 10 Mar 94.

FORM PTO-1449

INFORMATION DISCLOSURE CITATION IN AN APPLICATION

(Use several sheets if necessary)

Dock t Number	Applicati n Number
TUC920010022US1	09/977,159
Applicant G.A. Jaquette	
Filing Date October 11, 2001	**Gr up Art Unit** 2161

	ECMA Standardizing Information and Communication System, "Streaming Lossless Data Compression Algorithm - (SLDC), Se Draft, Dec 2000.
EXAMINER	**DATE CONSIDERED** 11/12/04

EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP § 609; Draw line through citation if not in conform and not considered. Include copy of this form with next communication to the applicant.